Journal of Symbolic Computation 46 (2011) 54–69

Contents lists available at ScienceDirect

Journal of Symbolic Computation

journal homepage: www.elsevier.com/locate/jsc

Solving genus zero Diophantine equations over number fields

Paraskevas Alvanos, Dimitrios Poulakis [1]

Department of Mathematics, Aristotle University of Thessaloniki, Thessaloniki 54124, Greece

ARTICLE INFO

Article history:
Received 24 September 2009
Accepted 2 September 2010
Available online 21 September 2010

Keywords:
Rational curves
Diophantine equations
Integral points
Valuations
Riemann–Roch space
Parametrization

ABSTRACT

Let K be a number field and $F(X, Y)$ an absolutely irreducible polynomial of $K[X, Y]$ such that the algebraic curve defined by the equation $F(X, Y) = 0$ is rational. In this paper we present practical algorithms for the determination of all solutions of the Diophantine equation $F(X, Y) = 0$ in algebraic integers of K.

1. Introduction

Let K be a number field, O_K the ring of integers of K and $\bar{K}$ an algebraic closure for K. Let $F(X, Y)$ be an absolutely irreducible polynomial of $K[X, Y]$ with $\deg F = N \geq 2$. We denote by C the affine algebraic curve associated to the equation $F(X, Y) = 0$ and we set

$$C(O_K) = \{(x, y) \in O_K^2 / F(x, y) = 0\}.$$

If L is a subfield of $\bar{K}$ with $L \supseteq K$, then we denote by $L(C)$ the function field of C over L. Furthermore, we denote by Σ_∞ the set of discrete valuation rings V of $\bar{K}(C)$ lying above the points of C at infinity.

Suppose that C has genus zero. When $|\Sigma_\infty| \geq 3$, the set $C(O_K)$ is finite (Maillet, 1918, 1919, Lang, 1978, Theorem 6.1, page 146, Lang, 1983, Chapter 8, Section 5). When $|\Sigma_\infty| \leq 2$, the set $C(O_K)$ may have infinitely many elements. In Alvanos et al. (2009), a necessary and sufficient condition for $C(O_K)$ to be infinite has been given.

E-mail addresses: paris14@math.auth.gr (P. Alvanos), poulakis@math.auth.gr (D. Poulakis).
[1] Tel.: +30 2310 997908.

0747-7171/$ – see front matter
doi:10.1016/j.jsc.2010.09.002

For $K = \mathbb{Q}$, algorithms have been presented in Poulakis and Voskos (2000, 2002) for the computation of elements of $C(\mathbb{Z})$ in cases where $|\Sigma_\infty| \geq 3$ and $|\Sigma_\infty| \leq 2$, respectively. In this paper, we study the general case where the rational curve C is defined over an arbitrary number field K and we give algorithms for the computation of elements of $C(O_K)$. All the steps of our algorithms can be achieved by using efficient algorithms implemented in the computational algebraic systems KASH (http://www.math.tu-berlin.de/~kant/), MAGMA (http://magma.maths.usyd.edu.au/magma/) and MAPLE. Note that our results can be adapted in the case of S-integers. Since there is no implementation for all necessary S-integer computations in a computational system, as for instance for the resolution of S-unit equations, we have preferred to restrict ourselves to the case of algebraic integers.

The algorithm developed in Poulakis and Voskos (2000) for the case $|\Sigma_\infty| \geq 3$ relies on the construction of a parametrization of C over $\mathbb{Q}$ and an efficient method for solving Thue equations over $\mathbb{Q}$. A method for solving Thue equations over a number field is given in Gaál and Pohst (2002) but it is not implemented in a computational system. Thus, the algorithm given in this paper for the case $|\Sigma_\infty| \geq 3$ is based on the construction of two functions f_1, f_2 on C defined over a finite extension M of K with their zeros and poles at infinity using the efficient algorithm of Hess (2002). Further, the functions f_1, f_2 satisfy an equality $c_1 f_1 + c_2 f_2 = 1$, where $c_1, c_2 \in M$. This reduces our problem to the resolution of a finite number of unit equations over M, a task which can be achieved by the efficient algorithm of Wildanger (2000).

The algorithm presented in Poulakis and Voskos (2002) for the case $|\Sigma_\infty| = 2$ is based on the construction of an appropriate parametrization of C over $\mathbb{Q}$ and on some divisibility relations or on the solution of a finite number of generalized Pell equations according to whether the elements of Σ_∞ are defined or not over $\mathbb{Q}$. In this paper we deal first with the case where the elements of Σ_∞ are defined over K generalizing the method of Poulakis and Voskos (2002). Our algorithm is based on the construction of an appropriate parametrization of C over K, on the computation of a maximal set of pairwise non associate elements of O_K of given norm, on the computation of a basis of the unit group of K and on some computations in the group of units of a quotient ring of O_K. In the case where the elements of Σ_∞ are not defined over K our approach is completely different from that of Poulakis and Voskos (2002). We reduce the problem to the same problem over a quadratic extension L of K such that the elements of Σ_∞ are defined over L and we work as in the previous case.

Finally, the algorithm given in Poulakis and Voskos (2002) for the case $|\Sigma_\infty| = 1$ is based on the construction of an appropriate parametrization of C over $\mathbb{Q}$ and the solution of some polynomial congruences. In this paper we generalize this approach.

The paper is organized as follows. In Sections 2 and 3, we recall some facts about the valuations and the divisors of the function fields of algebraic curves and we give some auxiliary lemmata and algorithms. In Section 4 we consider the case of rational curves with at least three valuations at infinity and we give an algorithm for computing their integral points. The cases of rational curves with two and one valuations are studied in Sections 5 and 6, respectively.

2. Valuations at infinity

Let L be a subfield of $\bar{K}$. We recall that the discrete valuation rings of the rational field $L(T)$ are of the form

$$V_{L,\infty} = \left\{ \frac{f(T)}{g(T)} : f(T), g(T) \in L[T],\ g(T) \neq 0,\ \deg f \leq \deg g \right\},$$

and for every irreducible polynomial $p(T) \in L[T]$, the ring

$$V_{L,p(T)} = \left\{ \frac{f(T)}{g(T)} : f(T), g(T) \in L[T],\ \gcd(f,g) = 1,\ p(T) \not| g(T) \right\}.$$

When $L = \bar{K}$, we simply set $V_\infty = V_{\bar{K},\infty}$ and $V_a = V_{\bar{K},T-a}$. Let V_P be the local ring of $\mathbb{P}^1$ at a point $P \in \mathbb{P}^1$. If $P = (a : 1)$, then $V_P = V_a$ and if $P = (1 : 0)$, then $V_P = V_\infty$, respectively.

Suppose now that $K \subseteq L$. Then we denote by Σ_L the set of all discrete valuation rings of $L(C)$ and by $\Sigma_{L,\infty}$ the set of rings $V \in \Sigma_L$ such that $V \cap L(T) = V_{L,\infty}$. If $L = \bar{K}$, then we put $\Sigma = \Sigma_{\bar{K}}$ and $\Sigma_\infty = \Sigma_{\bar{K},\infty}$.

Let $F_h(X, Y, Z)$ be the homogenization of $F(X, Y)$. We denote by $\tilde{C}$ the projective curve defined by the equation $F_h(X, Y, Z) = 0$ and by $\tilde{C}(L)$ the set of points of $\tilde{C}$ defined over L. Recall that the points $(a : b : 0)$ of the projective plane over $\bar{K}$ with $F_h(a, b, 0) = 0$ are called points of C at infinity. We denote by C_∞ the set of these points.

If A and B are local rings with $B \supset A$ and the maximal ideal of B contains the maximal ideal of A, then we say that B dominates A. If V dominates the local ring O_P of a point $P \in \tilde{C}(\bar{K})$, then we say that V is above P.

Suppose that $F(X, Y)$ is a constant times monic in Y. Then the homogeneous part of degree N of $F(X, Y)$ has the form $c \prod_{i=1}^{l} (Y - a_i X)^{m_i}$, where $a_1, \ldots, a_l$ are distinct elements of $\bar{K}$, $c \in K$ and $m_1 + \cdots + m_l = N$. It follows that $C_\infty = \{(1 : a_1 : 0), \ldots, (1 : a_l : 0)\}$. The function defined by $1/X$ on C has a zero at $(1 : a_i : 0)$ and so, it belongs to the maximal ideal of every discrete valuation ring above $(1 : a_i : 0)$ $(i = 1, \ldots, l)$. Hence the discrete valuation rings above the points of C_∞ are elements of Σ_∞. Suppose now that $V \in \Sigma_\infty$. Then V is above the local ring of a unique point P of C. If $P = (a, b)$, then $X - a \in V_\infty$ which is a contradiction. Hence P is a point at infinity. Therefore, in the case where $F(X, Y)$ is a constant times monic in Y, we have $V \in \Sigma_\infty$ if and only if V is above a point of C_∞. Otherwise, these two sets do not always coincide. For example, consider the curve C defined by the equation $XY = 1$. We have $\bar{K}(C) = \bar{K}(X)$ and so, V_∞ is the only element of Σ_∞. On the other hand, $C_\infty = \{(1 : 0 : 0), (0 : 1 : 0)\}$ and hence there are two discrete valuation rings above C_∞.

If $F(X, Y)$ is not a constant times monic in Y, then an affine change of cordinates $X = X' + aY'$, $Y = Y'$ for suitable $a \in O_K$ gives us the desired form. Furthermore, if we know the integral solutions of the equation $F(X' + aY', Y') = 0$, then we obtain very easily the integral solutions of $F(X, Y) = 0$. Thus, for the rest of the paper we suppose that $F(X, Y)$ is a constant times monic in Y. Thus, a point P of C_∞ has the form $P = (1 : a : 0)$ and Σ_∞ coincides with the set of discrete valuation rings above the elements of C_∞.

Let V be a discrete valuation ring of $K(C)$ and $\mathcal{M}$ its maximal ideal. The field $L = V/\mathcal{M}$ is a finite extension of K which is called the residue class field of V.

For every number field L we put $G_L = \mathrm{Gal}(\bar{K}/L)$. Let h be a polynomial with coefficients in $\bar{K}$. Then G_K acts on h by acting on its coefficients. Since every element of the coordinate ring $\bar{K}[C] = \bar{K}[X, Y]/(F)$ is well defined up to a polynomial vanishing on C and G_K takes the ideal (F) into itself, we have an action of G_K on $\bar{K}[C]$ and $\bar{K}(C)$. We denote the action of $\sigma \in G_K$ on $f \in \bar{K}(C)$ by $f \to f^\sigma$. We say that $V \in \Sigma$ is defined over L, if for every $\sigma \in G_L$ we have $V^\sigma = V$.

Now, we suppose that C is rational and there is a birational map $\phi : \mathbb{P}^1 \to \tilde{C}$ defined over K. Then ϕ induces a field isomorphism $\tilde{\phi} : \bar{K}(C) \to \bar{K}(T)$ given by the correspondence $f \mapsto f \circ \phi$ and defined over K.

Lemma 1. *Let V be a discrete valuation ring of $K(C)$ with residue class field L. Put $t = [L : K]$. Let $\sigma_1, \ldots, \sigma_t \in G_K$ $(i = 1, \ldots, t)$ be such that their restrictions on L give all the embeddings of L into $\bar{K}$. Then there is $W \in \Sigma$ such that the discrete valuation rings W^{σ_i} $(i = 1, \ldots, t)$ are all the elements of Σ with $W^{\sigma_i} \cap K(C) = V$. Furthermore, W^{σ_i} is defined over $\sigma_i(L)$.*

Proof. Suppose first that $\tilde{\phi}(V) = V_{K,\infty}$. Then $L = K$ and V_∞ is the only discrete valuation ring of $\bar{K}(X)$ with $V_\infty \cap K(X) = V_{K,\infty}$. It follows that there is only one element $W \in \Sigma$ with $W \cap K(C) = V$ and is defined over K.

Suppose now $\tilde{\phi}(V) = V_{K,p(X)}$, where $p(X)$ is an irreducible polynomial of $K[X]$. Let $\mathcal{M}$ be the maximal ideal of V. We have

$$L = V/\mathcal{M} \cong \tilde{\phi}(V)/\tilde{\phi}(\mathcal{M}) \cong K[X]/(p(X)).$$

Then $\deg p = t$. Let $a_1, \ldots, a_t$ be the roots of $p(X)$. The rings V_{a_i} $(i = 1, \ldots, t)$ are the only elements of Σ with $V_{a_i} \cap K(X) = V_{K,p(X)}$ and V_{a_i} is defined over $K(a_i)$ $(i = 1, \ldots, t)$. Hence, $V_i = \tilde{\phi}^{-1}(V_{a_i})$ $(i = 1, \ldots, t)$ are all the elements of Σ such that $V_i \cap K(C) = V$. Moreover, V_i is defined over $K(a_i)$ and we have $V_i = V_1^{\sigma_i}$, where $\sigma_i \in G_K$ $(i = 1, \ldots, t)$ and σ_1 is the identity. □

Let $P = (\rho : 1 : 0)$ be a point of C_∞. We can determine the set of elements of Σ_∞ above P as follows. If P is simple, then the only element of Σ_∞ above P is the local ring O_P. Suppose that P is singular and put $K(P) = K(\rho)$. Using the computational system MAGMA, we can easily compute the residue class fields $L_1, \ldots, L_s$ of all the elements of $\Sigma_{K(P),\infty}$ above P. Next, we compute the elements $U_1, \ldots, U_s$ of $\Sigma_{M,\infty}$ above P, where M is the normal closure of the composition of $L_1, \ldots, L_s$ over K. By Lemma 1, for every $i = 1, \ldots, s$ there is only one $\bar{U}_i \in \Sigma_\infty$ with $\bar{U}_i \cap M(C) = U_i$ and $\bar{U}_i$ is defined over M. Hence, $\bar{U}_1, \ldots, \bar{U}_s$ are all the elements Σ_∞ above P.

An alternative way to describe the elements of Σ_∞ is given in the following lemma.

Lemma 2. *Suppose that the birational map $\phi : \mathbb{P}^1 \to \tilde{C}$ is defined by the correspondence*

$$(S, T) \longmapsto (u(S, T), v(S, T), w(S, T)),$$

where $u(S, T)$, $v(S, T)$, $w(S, T)$ are homogeneous polynomials of $O_K[X, Y]$, of the same degree and with no common non-constant factor. Then we have the following:

(a) *The map ϕ is a birational morphism of $\mathbb{P}^1$ onto $\tilde{C}$ and $\deg u(S, T) = \deg v(S, T) = \deg w(S, T) = N$.*
(b) *If $(x : y : 1)$ is a non-singular point of $\tilde{C}(K)$, then there exist $s, t \in O_K$ such that $x = u(s, t)/w(s, t)$ and $y = v(s, t)/w(s, t)$.*
(c) *Let Z be the set of $(a : b) \in \mathbb{P}^1$ with $w(a, b) = 0$. Then the map*

$$\alpha : Z \longrightarrow \Sigma_\infty, \ P \longmapsto \tilde{\phi}^{-1}(V_P)$$

is a bijection.
(d) *If L is a finite extension of K and $P = (x : 1)$, then $x \in L$ if and only if $\tilde{\phi}^{-1}(V_x)$ is defined over L.*

Proof. The proof of (1)–(3) is essentially the same as the proofs of Lemmata 2.1 and 2.2 of Poulakis and Voskos (2000). We shall prove (4). Suppose that $a \in L$. Then the ring V_a is defined over L. Since the map ϕ is defined over K, we deduce that the ring $\tilde{\phi}^{-1}(V_a)$ is also defined over L. Conversely, suppose that $\tilde{\phi}^{-1}(V_a)$ is defined over L. Since $\tilde{\phi}$ is rational over K, it follows that V_a is defined over L. Then, for every $\sigma \in G_L$ we have $V_a^\sigma = V_a$ and so, there are $f_\sigma(X), g_\sigma(X) \in \bar{K}[X]$ such that $X - \sigma(a) = f_\sigma(X)(X - a)/g_\sigma(X)$ and $X - a \not| g_\sigma(X)$. It follows that $\sigma(a) = a$, for every $\sigma \in G_L$ and hence $a \in L$. □

3. Divisors

The divisor group of C, denoted by $\mathrm{Div}(C)$, is the free abelian group generated by the elements of Σ. Thus a divisor $D \in \mathrm{Div}(C)$ is a formal sum $D = \sum_{V \in \Sigma} n_V V$, where $n_V \in \mathbb{Z}$ and $n_V = 0$ for all but finitely $V \in \Sigma$. The degree of D is defined by $\deg D = \sum_{V \in \Sigma} n_V$. Let $f \in \bar{K}(C) \setminus \{0\}$ and $V \in \Sigma$. We denote by $\mathrm{ord}_V(f)$ the order of f at V. We say that V is a zero of f if $\mathrm{ord}_V(f) > 0$ and a pole if $\mathrm{ord}_V(f) < 0$. Let $D = \sum_{V \in \Sigma} n_V V$ be a divisor. We associate to D the set of functions

$$L(D) = \{f \in \bar{K}(C) \setminus \{0\} : \ \mathrm{ord}_V(f) \geq -n_V, \forall\, V \in \Sigma\} \cup \{0\}.$$

If $\sigma \in G_K$, then we put $D^\sigma = \sum_{V \in \Sigma} n_V V^\sigma$. Let L be a finite extension of K. We say that D is defined over L, if for every $\sigma \in G_L$ we have $D^\sigma = D$.

Let $V, W \in \Sigma_\infty$. Since C is rational, the Riemann–Roch theorem implies $\dim L(V - W) = 1$. Suppose that the divisor $V - W$ is defined over the finite extension M of K. By Schmidt (1991, Theorem B2), there is a function $f \in L(V - W)$ defined over M. So, the zeros and poles of f are in Σ_∞. Let x and y be the coordinate functions on C. Since $\deg f = 1$, we have $M(C) = M(f)$ and hence $[M(x, f) : M(x)] = N$. Thus, there are $a_0(x), \ldots, a_N(x) \in M[x]$ such that

$$a_0(x) f^N + a_1(x) f^{N-1} + \cdots + a_N(x) = 0.$$

Suppose that $a_0(x) \notin M$. The zeros of $a_0(x)$ are not in Σ_∞. It follows that f has a pole outside of Σ_∞ which is a contradiction (recall that the set of discrete valuation rings above C_∞ coincides with Σ_∞). Hence $a_0(x) \in M$ and so, f is an integral element over $M[x]$. Similarly, we see that $1/f$ is also an integral element over $M[x]$.

Next, we describe an algorithm that for given $f \in L(V - W)$, computes $\alpha, \beta \in O_M$ such that αf and β/f are integral elements over $O_M[x]$.

The Algorithm DENOMINATORS

Input: $a(X, Y), b(X, Y) \in M[X, Y]$ such that $a(X, Y)/b(X, Y)$ defines a function $f \in L(V - W)$.
Output: $\alpha, \beta \in O_M$ such that αf and β/f are integral elements over $O_M[x]$.

(1) Compute the resultant $R(X, T)$ of $G(X, Y, T) = b(X, Y)T - a(X, Y)$ and $F(X, Y)$ with respect to Y.
(2) Factorize $R(X, T)$ over M.
(3) Determine the irreducible factor $R_1(X, T)$ of $R(X, T)$ with $R_1(x, f) = 0$. We have

$$R_1(x, T) = A_0(x)T^N + A_1(x)T^{N-1} + \cdots + A_N(x),$$

where $A_0(x), A_N(x) \in M$ and $A_j(x) \in M[x]$ $(j = 1, \ldots, N - 1)$.
(4) Compute $\alpha, \beta \in O_M$ such that $\alpha^i A_i(x)/A_0(x) \in O_M[x]$ $(i = 1, \ldots, N)$ and $\beta^{N-i} A_i(x)/A_N(x) \in O_M[x]$ $(i = 0, \ldots, N - 1)$.
(5) Output α, β and stop.

Proof of correctness. The functions x, y and f satisfy $F(x, y) = G(x, y, f) = 0$ and so $R(x, f) = 0$. Thus the irreducible polynomial of f over $M(x)$ is $R_1(x, T)$. Since f is integral over $M[x]$, we have $A_0(x) \in M$. The coefficient of T^i of the monic polynomial $(\alpha^N/A_0(X))R_1(x, T/\alpha)$ is $\alpha A_i(x)/A_0(x) \in O_M[x]$ $(i = 1, \ldots, N)$. The function αf is a root of this polynomial and so, αf is integral over $O_M[x]$. Similarly, the irreducible polynomial of $1/f$ over $M(x)$ is $T^N R_1(x, 1/T)$ and so, we deduce, as previously, that β/f is integral over $O_M[x]$.

4. Curves with $|\Sigma_\infty| \geq 3$

In this section we assume $|\Sigma_\infty| \geq 3$ and we describe an algorithm for the computation of all elements of $C(O_K)$. If L is a finite extension of K we denote by $N_{L/K}$, as usually, the norm map from L to K. In the case where $K = \mathbb{Q}$ we denote this map by N_L.

The Algorithm INTEGRAL-POINTS3

Input: $C : F(X, Y) = 0$ and $V_1, V_2, V_3 \in \Sigma_\infty$.
Output: The elements of $C(O_K)$.

(1) Compute the singular points of C.
(2) Determine number fields M_i with $K \subseteq M_i \subseteq \bar{K}$ and $a_i(X, Y) \in M_i[X, Y]$, $b_i(X) \in M_i[X]$ $(i = 1, 2)$ with $\deg_Y a_i(X, Y) < N$ such that $a_i(X, Y)/b_i(X)$ defines a function $f_i \in L(V_3 - V_i)$.
(3) Using the algorithm DENOMINATORS, compute $\alpha_i, \beta_i \in O_{M_i}$ such that $\alpha_i f_i$ and β_i/f_i are integral elements over $O_{M_i}[x]$ $(i = 1, 2)$.
(4) Determine maximal sets A_i $(i = 1, 2)$ of pairwise non associate elements of O_{M_i} with norm dividing $N_{M_i}(\alpha_i \beta_i)$.
(5) Let M be the normal closure of the composition of M_1 and M_2 over K. Determine $c_1, c_2 \in M$ such that $c_1 f_1 + c_2 f_2 = 1$.
(6) For every $(k_1, k_2) \in A_1 \times A_2$, determine the set of solutions $S(k_1, k_2)$ of the unit equation

$$(c_1 k_1/\alpha_1)U_1 + (c_2 k_2/\alpha_2)U_2 = 1.$$

(7) For every $(k_1, k_2) \in A_1 \times A_2$ and $(u_1, u_2) \in S(k_1, k_2)$, compute the resultant $R_{k_1,u_1}(X)$ of $F(X, Y)$ and $\alpha_1 a_1(X, Y) - k_1 u_1 b_1(X)$ with respect to Y and determine the set S of $v \in O_K$ such that $R_{k_1,u_1}(v) = 0$ for some $(k_1, k_2) \in A_1 \times A_2$ and $(u_1, u_2) \in S(k_1, k_2)$.
(8) Determine all the pairs $(v, w) \in C(O_K)$ with $v \in S$.
(9) Output the singular integral points defined over K and the pairs computed in the previous step, and stop.

Proof of correctness. Let M_i be the smallest field of definition of the divisor $V_3 - V_i$ $(i = 1, 2)$. Since C is rational, Riemann–Roch theorem implies that the dimension of $L(V_3 - V_i)$ is 1. By Schmidt (1991, Theorem B2), there are polynomials $a_i(X, Y) \in M_i[X, Y]$, $b_i(X) \in M_i[X]$ $(i = 1, 2)$ with $\deg_Y a_i(X, Y) < N$ such that $a_i(X, Y)/b_i(X)$ defines a function $f_i \in L(V_3 - V_i)$ $(i = 1, 2)$. The zeros and poles of f_i are at infinity, and so, f_i and $1/f_i$ are integral elements over $M[x]$. We consider $\alpha_i, \beta_i \in O_{M_i}$ such that $\alpha_i f_i$ and β_i/f_i are integral elements over $O_{M_i}[x]$ $(i = 1, 2)$.

Let $(v, w) \in C(O_K)$ be a non-singular point. Then the elements $\alpha_i f_i(v, w)$ and $\beta_i/f_i(v, w)$ are integral over O_{M_i} $(i = 1, 2)$. Since O_{M_i} is integrally closed, it follows that $\alpha_i f_i(v, w)$, $\beta_i/f_i(v, w) \in O_{M_i}$ $(i = 1, 2)$. Since

$$\frac{\alpha_i\beta_i}{\alpha_i f_i(v, w)} = \frac{\beta_i}{f_i(v, w)} \in O_{M_i},$$

we deduce that $N_{M_i}(\alpha_i f_i(v, w))$ divides $N_{M_i}(\alpha_i\beta_i)$ $(i = 1, 2)$. Let A_i be a maximal set of pairwise non associate elements of O_{M_i} with norm dividing $N_{M_i}(\alpha_i\beta_i)$ $(i = 1, 2)$. Then $\alpha_i f_i(v, w) = k_i u_i$, where $k_i \in A_i$ and u_i is a unit of O_{M_i} $(i = 1, 2)$.

Let M be the composition of M_1 and M_2. By the Riemann–Roch theorem the dimension of $L(V_3)$ is 2. Thus, there are $c_1, c_2 \in M$ such that $c_1 f_1 + c_2 f_2 = 1$. Thus, we have

$$(c_1 k_1/\alpha_1)u_1 + (c_2 k_2/\alpha_2)u_2 = 1.$$

Since $\deg_Y a_1(X, Y) < N$ and $F(X, Y)$ is absolutely irreducible, it follows that $F(X, Y)$ does not divide $\alpha_1 a_1(X, Y) - k_1 u_1 b_1(X)$. So, the resultant $R_{k_1,u_1}(X)$ of $F(X, Y)$ and $\alpha_1 a_1(X, Y) - k_1 u_1 b_1(X)$ with respect to Y is not zero and v is a root of $R_{k_1,u_1}(X)$.

Note that there are efficient algorithms which can carry out all the steps of the previous algorithm, and are implemented in the computational algebraic systems MAGMA and KASH. Next, we give an example of application of our algorithm.

Example 1. Let

$$F(X, Y) = 3X^4 - (1 + \theta)Y^4 - 4\theta X^2Y^2 - 9X^3 + 8\theta XY^2 + 9X^2 - 4\theta Y^2 - 3X,$$

where $\theta = (-1 + \sqrt{-3})/2$. The solutions of the equation $F(X, Y) = 0$ in $\mathbb{Z}[\theta]$ are

$$(X, Y) = (0, 0), (1, 0), (0, -1 + \sqrt{-3}), (0, 1 - \sqrt{-3}).$$

Proof. The equation $F(X, Y) = 0$ defines a rational curve C. The only singular point of C is $(1, 0)$. Put $c = \sqrt{-3\theta - 3}$. The points at infinity of C are $P_1 = (1 : c : 0)$, $P_2 = (1 : -c : 0)$, $P_3 = (1 : -\theta : 0)$ and $P_4 = (1 : \theta : 0)$. They are all simple and defined over the field $K = \mathbb{Q}(c)$. Thus, the local ring $V_i = O_{P_i}$ of C at P_i $(i = 1, 2, 3)$ is a discrete valuation ring. Since C has genus zero, we have $\dim L(V_1 - V_i) = 1$ $(i = 2, 3)$. The nonzero functions

$$f_1 = \frac{-2c^3y^3 - 6(c^2 + 3)(x - 1)y^2 - 2c(c^2 + 3)(x - 1)^2y + 9(-2x + 1)(x - 1)^2}{9(x - 1)^2}$$

and

$$f_2 = \frac{(-c^3 + 9)y^3 - 3\sigma(x - 1)y^2 - c\sigma(x - 1)^2y + (3c^3x - 9x + 9)(x - 1)^2}{9(x - 1)^2},$$

where $\sigma = c^2 + 3c + 3$, belong to $L(V_1 - V_3)$ and $L(V_1 - V_2)$, respectively.

Now, we shall apply the algorithm DENOMINATORS. Let $R_1(X, T)$ and $R_2(X, T)$ be the resultants with respect to Y of polynomials $G_1(X, Y, T) = (X-1)^2 f_1(X, Y) - T(X-1)^2, F(X, Y)$ and $G_2(X, Y, T) = (X - 1)^2 f_2(X, Y) - T(X - 1)^2, F(X, Y)$, respectively. We have

$$R_1(X, T) = (X - 1)^8 I_1(X, T), \qquad R_2(X, T) = (X - 1)^8 I_2(X, T),$$

where

$$I_1(X, T) = T^4 - (8X - 12)T^3 + (32X - 26)T^2 - (8X - 12)T + 1$$

and

$$I_2(X,T) = T^4 + 1/3((4c^3-12)X + (-8c^3+12))T^3 - 1/3((16c^3-60)X + (16c^3-6))T^2 - 1/3((4c^3-36)X + (8c^3+36))T + 9$$

are irreducible over K. It follows that $I_1(x,T)$ and $I_2(x,T)$ are the irreducible polynomials of f_1 and f_2, respectively, over $K(x)$. Let O_K be the ring of algebraic integers of K. We see that f_1 and f_2 are integral over $O_K[x]$. The irreducible polynomials of $1/f_1$ and $1/f_2$ over $K(x)$ are $T^4 I_1(x, 1/T)$ and $T^4 I_2(x, 1/T)/9$ respectively. Hence $1/f_1$ and $9/f_2$ are integral over $O_K[x]$.

A maximal set of pairwise non associate elements of O_K with norm dividing 9^4 is

$$A = \{1, c, c^2, c^3, -3c^2 - 9\}.$$

Now, we shall compute $c_1, c_2 \in K$ such that $c_1 f_1 + c_2 f_2 = 1$. The couples $P_1 = (0,0)$ and $P_2 = (0, -1+\sqrt{-3})$ are points on C. We have

$$f_1(P_1) = f_2(P_1) = 1, \qquad f_1(P_2) = 4\sqrt{3} - 7, \qquad f_2(P_2) = -2\sqrt{3} + 3.$$

We solve the linear system

$$c_1 f_1(P_1) + c_2 f_2(P_1) = 1, \qquad c_1 f_1(P_2) + c_2 f_2(P_2) = 1$$

and we obtain $c_1 = \sqrt{3} + 2$ and $c_2 = -\sqrt{3} - 1$.

An integral basis for the field K is given by the elements $\omega_0 = 1$, $\omega_1 = c$, $\omega_2 = c^2/3$ and $\omega_3 = (-3c + c^3)/9$. Thus, we represent an algebraic integer of K, $z = \sum_{i=0}^{3} z_i \omega_i$, where $z_i \in \mathbb{Z}$ ($i = 0, 1, 2, 3$), by $z = [z_0, z_1, z_2, z_3]$.

We denote by $S(k)$ the set of solutions of the unit equation

$$c_1 U_1 + c_2 k U_2 = 1,$$

where $k \in A$. For $k = c^2, -3c^2 - 9$ the set $S(k)$ is empty. Further, we have

$$S(c) = \{([-7, -4, 0, -12], [0, -2, 2, -3]),\ ([-1, 0, 0, 0], [0, 0, 1, 0])\}$$

and

$$S(c^3) = \{([-97, -56, 0, -168], [7, 4, 0, 12]),\ ([-7, 4, 0, 12], [2, -1, 0, -3])\}.$$

Finally, the elements of $S(1)$ are given in the following table:

$([-1,-4,3,-7],[1,2,-1,4])$	$([-4,1,-3,-2],[2,0,1,2])$
$([0,-1,1,-2],[1,1,0,2])$	$([1,-2,2,-2],[0,1,-1,2])$
$([-1,0,-1,-1],[1,0,0,1])$	$([1,0,0,0],[1,0,0,0])$
$([1,0,1,1],[0,1,0,2])$	$([-1,2,-2,2],[1,0,1,1])$
$([0,1,-1,2],[0,0,0,1])$	$([4,-1,3,2],[-1,1,-1,1])$
$([1,4,-3,7],[0,-1,1,-1])$	$([7,4,0,12],[-2,-1,0,-3])$

For every $k \in A$ and $(u_1, u_2) \in S(k)$, we compute the resultant $R_{k,u_1}(X)$ of $F(X,Y)$ and $9(X-1)^2 f_1(X,Y) - u_1 9(X-1)^2$ with respect to Y. We find the roots of the polynomials $R_{k,u_1}(X)$ and finally we deduce that the solutions of the equation $F(X,Y) = 0$ in $\mathbb{Z}[\theta]$ are $(0,0)$, $(1,0)$, $(0, -1+\sqrt{-3})$, $(0, 1-\sqrt{-3})$. □

5. Curves with $|\Sigma_\infty| = 2$

In this section we suppose that the curve C has $|\Sigma_\infty| = 2$. If A is a commutative ring, then we denote by A^* its group of units. By Lemma 2, the elements of Σ_∞ are either both defined or both not defined over K. First, we consider the case that both elements of Σ_∞ are defined over K. The following algorithm computes the elements of $C(O_K)$.

The Algorithm INTEGRAL-POINTS2A

Input: $C : F(X, Y) = 0$ with $\Sigma_\infty = \{V_1, V_2\}$ and V_1, V_2 are defined over K.
Output: The elements of $C(O_K)$.

(1) Determine the singular points of $C(O_K)$.
(2) Find homogeneous polynomials $p(U, V), q(U, V) \in O_K[U, V]$ of degree N and $A \in O_K \setminus \{0\}$ such that the correspondence

$$(U, V) \longmapsto (p(U, V), q(U, V), AU^\mu V^\nu),$$

defines a birational morphism $\psi : \mathbb{P}^1 \to \tilde{C}$ over K. If there are no such polynomials, then $C(O_K)$ contains only the points obtained in Step 1. Else, go to the next step.
(3) Let

$$p(U, V) = \sum_{i=0}^{N} a_i U^{N-i} V^i, \qquad q(U, V) = \sum_{i=0}^{N} b_i U^{N-i} V^i$$

and $a_0 = a_0' A_0$, $b_0 = b_0' B_0$, where $a_0', b_0' \in \mathbb{Z}$ and A_0 (respectively B_0) is 1 or is not a rational integer. Put $E = \mathbb{Q}(A_0)$ and $L = \mathbb{Q}(B_0)$ and compute $\delta_0 = \gcd(a_0' N_E(A_0), b_0' N_L(B_0))$ and $\delta_N = \gcd(N_K(a_N), N_K(b_N))$.
(4) Compute the resultant R of the polynomials

$$\tilde{p}(T) = \sum_{i=0}^{N} a_i \delta_0^i T^{N-i}, \qquad \tilde{q}(T) = \sum_{i=0}^{N} b_i \delta_0^i T^{N-i}.$$

If $N_K(A\delta_0^\nu) \nmid N_K(R)$, then the elements of $C(O_K)$ are those computed in Step 1. Otherwise, go to the next step.
(5) Compute a maximal set M of pairwise non associate elements $t \in O_K$ such that $N_K(t) | \gcd(\delta_0^{N \deg K} \delta_N, N_K(R))$.
(6) Compute a basis, $\zeta, \epsilon_1, \ldots, \epsilon_r$ for the unit group O_K^* of K, where ζ is a κ-th root of unity and $\epsilon_1, \ldots, \epsilon_r$ a basis for the free part of O_K^*.
(7) For every $t \in M$, compute the order $\tau(i, t)$ of the class of ϵ_i in $(O_K/(\delta_0^\nu A t^\mu))^*$.
(8) For every $t \in M$, determine the set $H(t)$ of units $\eta = \zeta^l \epsilon_1^{l_1} \cdots \epsilon_r^{l_r}$ with $0 \le l < \kappa$ and $0 \le l_i < \tau(i, t)$ $(i = 1, \ldots, r)$ such that $\tilde{p}(t\eta)/(\delta_0^\nu A(t\eta)^\mu)$ and $\tilde{q}(t\eta)/(\delta_0^\nu A(t\eta)^\mu)$ are in O_K.
(9) For every $t \in M$ let $\Theta(t) = \{\epsilon_1^{\tau(1,t)z_1} \cdots \epsilon_r^{\tau(r,t)z_r} / z_1, \ldots, z_r \in \mathbb{Z}\}$. The elements of $C(O_K)$ are the points computed in Steps 1 and the pairs

$$\left(\frac{\tilde{p}(t\eta\epsilon)}{\delta_0^\nu A(t\eta\epsilon)^\mu}, \frac{\tilde{q}(t\eta\epsilon)}{\delta_0^\nu A(t\eta\epsilon)^\mu} \right)$$

where $\eta \in H(t)$ and $\epsilon \in \Theta(t)$.

Proof of correctness. Suppose that C has no non-singular point over K. Thus, if the equation $F(X, Y) = 0$ has a solution $(x, y) \in O_K^2$, then (x, y) is a singular point of C. If C has a non-singular point over K, then there are homogeneous polynomials $u(S, T)$, $v(S, T)$ and $w(S, T)$ in $O_K[S, T]$ of the same degree with no common non-constant factor such that the correspondence

$$(S, T) \longmapsto (u(S, T), v(S, T), w(S, T))$$

defines a birational map $\phi : \mathbb{P}^1 \to \tilde{C}$ over K. By Lemma 2(a), we have that ϕ is a birational morphism of $\mathbb{P}^1$ onto C and $\deg u(S, T) = \deg v(S, T) = \deg w(S, T) = N$. Since $|\Sigma_\infty| = 2$, Lemma 2(c) implies $w(S, T) = a(bS + cT)^\mu (dS + eT)^\nu$, where $bS + cT$, $dS + eT$ are not proportional and $\mu \ge 1, \nu \ge 1$ with $\mu + \nu = N$.

Put $U = bS + cT$, $V = dS + eT$ to ϕ and determine a birational morphism $\psi : \mathbb{P}^1 \to \tilde{C}$ over K given by the correspondence

$$(U, V) \longmapsto (p(U, V), q(U, V), AU^\mu V^\nu),$$

where

$$p(U,V)=\sum_{i=0}^{N}a_iU^{N-i}V^i,\qquad q(U,V)=\sum_{i=0}^{N}b_iU^{N-i}V^i$$

are homogeneous polynomials in $O_K[U,V]$ of degree N and $A\in O_K\setminus\{0\}$. Since $\gcd(p(U,V),q(U,V),AU^\mu V^\nu)=1$, we have $(a_0,b_0)\neq(0,0)$ and $(a_N,b_N)\neq(0,0)$.

Let $(x,y)\in O_K^2$ be a non-singular point of C. By Lemma 2(b), there exist $u,v\in O_K\setminus\{0\}$ such that $x=p(u,v)/Au^\mu v^\nu$ and $y=q(u,v)/Au^\mu v^\nu$. Putting $s=u/v$, we get $x=p(s,1)/As^\mu$ and $y=q(s,1)/As^\mu$, whence we obtain $a_0s,b_0s\in O_K$.

Let $a_0=a_0'A_0$, $b_0=b_0'B_0$, where $a_0',b_0'\in\mathbb{Z}$ and A_0 (respectively B_0) is 1 or is not a rational integer. If $E=\mathbb{Q}(A_0)$ and $L=\mathbb{Q}(B_0)$, then we put $\delta_0=\gcd(a_0'N_E(A_0),b_0'N_L(B_0))$. Since $a_0'N_E(A_0)s,b_0'N_L(B_0)s\in O_K$, we deduce that $\delta_0s\in O_K$. We set $t=\delta_0s$ and

$$\tilde p(T)=\sum_{i=0}^{N}a_i\delta_0^iT^{N-i},\qquad \tilde q(T)=\sum_{i=0}^{N}b_i\delta_0^iT^{N-i}.$$

Further, we consider the map $\alpha:\mathbb{A}^1\setminus\{0\}\to\tilde C$ defined by

$$\alpha(a)=\left(\frac{\tilde p(a)}{A\delta_0^\nu a^\mu},\frac{\tilde q(a)}{A\delta_0^\nu a^\mu}\right)$$

for every $a\in\mathbb{A}^1\setminus\{0\}$.

Let R be the resultant of $\tilde p(T)$ and $\tilde q(T)$. Then, there are $f(T),g(T)\in O_K[T]$ such that

$$R=f(T)\tilde p(T)+g(T)\tilde q(T).$$

Since $(x,y)=\alpha(t)\in C(O_K)$, we have $A\delta_0^\nu t^\mu\mid\tilde p(t)$ and $A\delta_0^\nu t^\mu\mid\tilde q(t)$, whence $t\mid\delta_0^Na_N$ and $t\mid\delta_0^Nb_N$. If we put $\delta_N=\gcd(N_K(a_N),N_K(b_N))$, then we have $N_K(t)\mid\delta_0^{N\deg K}\delta_N$. Furthermore, we obtain $A\delta_0^\nu t^\mu\mid R$. Thus $N_K(A\delta_0^\nu)\mid N_K(R)$ and $N_K(t)\mid\gcd(N_K(R),\delta_0^{N\deg K}\delta_N)$.

Let M be a maximal set of pairwise non associate elements $z\in O_K$ such that $N_K(z)\mid\gcd(\delta_0^{N\deg K}\delta_N,N_K(R))$. Then $t=z\eta$, where $z\in M$ and $\eta\in O_K^*$. Further, if $z\in M$ and $\eta\in O_K^*$ are such that $\alpha(z\eta)\in C(O_K)$ and $\eta'\in O_K^*$ with $\eta\equiv\eta'\pmod{A\delta_0^\nu z^\mu}$, then $\alpha(z\eta')\in C(O_K)$. Let $\zeta,\epsilon_1,\dots,\epsilon_r$ be a basis for the unit group O_K^*, where ζ is a κ-th root of unity and $\epsilon_1,\dots,\epsilon_r$ a basis for the free part of O_K^*. For every $z\in M$, we denote by $\tau(i,z)$ the order of the class of ϵ_i in $(O_K/(\delta_0^\nu Az^\mu))^*$. Thus, we have $\epsilon_1^{l_1}\cdots\epsilon_r^{l_r}\equiv\epsilon_1^{k_1}\cdots\epsilon_r^{k_r}\pmod{A\delta_0^\nu z^\mu}$ if and only if $l_i\equiv k_i\pmod{\tau(i,z)}$ $(i=1,\dots,r)$. Therefore, if $\alpha(z\zeta^l\epsilon_1^{l_1}\cdots\epsilon_r^{l_r})\in C(O_K)$, where $z\in M$, $0\le l<\kappa$ and $0\le l_i<\tau(i,t)$ $(i=1,\dots,r)$, then $\alpha(z\zeta^l\epsilon_1^{l_1+z_1\tau(1,z)}\cdots\epsilon_r^{l_r+z_r\tau(r,z)})\in C(O_K)$ for every $z_1,\dots,z_r\in\mathbb{Z}$ and the points of $C(O_K)$ obtained in this manner are all the simple points of $C(O_K)$.

The steps of the previous algorithm can be carried out by KASH, MAGMA and MAPLE.

Example 2. Let $a=(1+\sqrt{5})/2$ and

$$\begin{aligned}F(X,Y)\ &=-8aX^3+(16a+12)X^2Y-(8a+24)XY^2+12Y^3\\&\quad+(8a+6)X^2-(8a+24)XY+18Y^2-(2a+6)X+9Y+17a-26.\end{aligned}$$

The solutions of the equation $F(X,Y)=0$ in $\mathbb{Z}[a]$ are

$$(X,Y)=\left(\frac{(6a+3)a^{9z}+(13-8a)}{2a^{6z}},\frac{(6a+4)a^{9z}-a^{6z}+(13-8a)}{2a^{6z}}\right),$$

where $z\in\mathbb{Z}$.

Proof. Denote by C the affine curve defined by $F(X,Y)=0$ and by $\tilde C$ its projective closure. The ring of integers of $K=\mathbb{Q}(\sqrt{5})$ is $\mathbb{Z}[a]$ and the unit group of $\mathbb{Z}[a]$ is generated by -1 and a. The only singular point of $\tilde C$ is $(1:1:0)$. A parametrization of $\tilde C$ is given by the birational morphism

$$\phi:\mathbb{P}^1\longrightarrow\tilde C,\ (s:t)\longmapsto(u(s,t):v(s,t):w(s,t)),$$

where

$$u(s,t) = 61(5-7a)[-(144+204a)t^3 + (216+306a)t^2s - (108+153a)ts^2 + 59s^3],$$
$$v(s,t) = 59(4-7a)[-(120+208a)t^3 + (174+326a)t^2s - (170a+84)ts^2 + 61s^3],$$
$$w(s,t) = 3599s(2t-s)^2.$$

Setting $z = s$, $w = 2t - s$, we obtain the following birational morphism

$$\psi : \mathbb{P}^1 \longrightarrow \tilde{C},\ (z:w) \longmapsto (\alpha(z,w) : \beta(z,w) : \gamma(z,w)),$$

where

$$\alpha(z,w) = (6a+3)z^3 + (13-8a)w^3,$$
$$\beta(z,w) = (6a+4)z^3 - z^2w + (13-8a)w^3,$$
$$\gamma(z,w) = 2z^2w.$$

We have $\gcd(N_K(6a+3), N_K(6a+4)) = \gcd(-9,4) = 1$ and $N_K(13-8a) = 1$. The resultant of polynomials $\alpha(T,1)$ and $\beta(T,1)$ is

$$R = 128a^3 - 1440a^2 + 3666a - 2704.$$

Since $2|R$, we continue to the next steps of our algorithm. A maximal set of pairwise non associate elements $t \in \mathbb{Z}[a]$ such that $N_K(t) = \pm 1$ is formed by 1 and a. Since a is a unit in $\mathbb{Z}[a]$ we have only the quotient ring $\mathbb{Z}[a]/(2)$. The order of a in $(\mathbb{Z}[a]/(2))^*$ is 3. For $i = 0, 1, 2$, we compute the quantities

$$\frac{(6a+3)a^{3i} + (13-8a)}{2a^{2i}}, \qquad \frac{(6a+4)a^{3i} - a^{2i} + (13-8a)}{2a^{2i}}$$

and we see that only for $i = 0$ they are in $\mathbb{Z}[a]$. The result follows. □

Now, we shall present an algorithm for the case where the elements of Σ_∞ are not defined over K. For this purpose we need the following auxiliary algorithm which computes a basis for the subgroup G of O_L^* consisting of $\eta \in O_L^*$ with $N_{L/K}(\eta) = 1$. We denote by $\mathcal{N}$ the restriction of the norm $N_{L/K}$ on O_L^*.

The Algorithm RELATIVE-UNITS

Input: A number field K and a finite extension L of K.
Output: A basis $\zeta, \epsilon_1, \ldots, \epsilon_r$ for the group G, where ζ is a κ-th root of unity and $\epsilon_1, \ldots, \epsilon_r$ a basis for the free part of G.

(1) Compute a basis $e_1, \ldots, e_r$ of the free part of O_L^*.
(2) Compute the group $H = \langle \mathcal{N}(e_1), \ldots, \mathcal{N}(e_r) \rangle$.
(3) Compute a basis $\zeta, \epsilon_1, \ldots, \epsilon_r$ for the kernel $Ker(\mathcal{N})$ of the morphism $\mathcal{N} : O_L^* \to H$, where ζ is a κ-th root of unity and $\epsilon_1, \ldots, \epsilon_r$ a basis for the free part of $Ker(\mathcal{N})$.
(4) Output $\zeta, \epsilon_1, \ldots, \epsilon_r$.

The steps of the previous algorithm can be achieved by MAGMA.

The following algorithm computes the integral solutions of $F(X,Y) = 0$ over K in the case where the two elements of Σ_∞ are not defined over K. Note that the generalized Pell equation has this property.

The Algorithm INTEGRAL-POINTS2B

Input: $C : F(X,Y) = 0$ with $\Sigma_\infty = \{V_1, V_2\}$ and V_1, V_2 are not defined over K.
Output: The elements of $C(O_K)$.

(1) Determine the singular points of $C(O_K)$.
(2) Find homogeneous polynomials $u(S,T), v(S,T), w(S,T) \in O_K[X,Y]$ of degree N with no common non-constant factor and $w(S,T) = k(aS^2 + bST + cT^2)^{N/2}$, where $\delta = b^2 - 4ac$ is not a square in K, such that the correspondence

$$(S,T) \longmapsto (u(S,T), v(S,T), w(S,T))$$

defines a birational morphism $\phi : \mathbb{P}^1 \to \tilde{C}$ over K. If there are not such polynomials, then the only elements of $C(O_K)$ are the points obtained in Step 1. Else, go to the next step.
(3) Let $L = K(\sqrt{\delta})$. Apply the change of coordinates $Z = 2aS + (b + \sqrt{\delta})T$, $W = 2aS + (b - \sqrt{\delta})T$ and obtain a birational morphism $\omega : \mathbb{P}^1 \to \tilde{C}$ over L given by the correspondence

$$(Z,W) \longmapsto (p(Z,W), q(Z,W), B(ZW)^{N/2}),$$

where $B \in O_L$ with $B | A2^N \delta^{N/2}$ and

$$p(Z,W) = \sum_{i=0}^{N} a_i Z^{N-i} W^i, \qquad q(Z,W) = \sum_{i=0}^{N} b_i Z^{N-i} W^i$$

are homogeneous polynomials in $O_L[Z,W]$ of degree N.
(4) Let $a_0 = \delta_1 A_1$, $b_0 = \delta_2 A_2$, where $\delta_i \in \mathbb{Z}$ and $A_i = 1$ or $A_i \notin \mathbb{Q}$, and $L_i = \mathbb{Q}(A_i)$ $(i = 1, 2)$. Compute $\Delta = \gcd(\delta_1 N_{L_1}(A_1)), \delta_2 N_{L_2}(A_2))$.
(5) Compute the resultant R of polynomials

$$\tilde{p}(T) = \sum_{i=0}^{N} a_i \Delta^i T^{N-i}, \qquad \tilde{q}(T) = \sum_{i=0}^{N} b_i \Delta^i T^{N-i}.$$

If $N_L(B\Delta^{N/2}) \not| N_L(R)$, then all the elements of $C(O_K)$ are those computed in Step 1. Otherwise, go to the next step.
(6) Compute a maximal set M of pairwise non associate elements $z \in O_L$ such that $N_{L/K}(z) = \Delta^2$.
(7) Let G be the subgroup of O_L^* consisting of $\eta \in O_L^*$ with $N_{L/K}(\eta) = 1$. Using the algorithm RELATIVE-UNITS, compute a basis $\zeta, \epsilon_1, \ldots, \epsilon_r$ for the unit group G, where ζ is a κ-th root of unity and $\epsilon_1, \ldots, \epsilon_r$ a basis for the free part of G.
(8) For every $t \in M$, compute the order $\tau(i,t)$ of the image of the class of ϵ_i in $(O_K/B(\Delta t)^{N/2})^*$.
(9) For every $t \in M$, determine the set $H(t)$ of units $\eta = \zeta^l \epsilon_1^{l_1} \cdots \epsilon_r^{l_r}$ with $0 \le l < \kappa$ and $0 \le l_i < \tau(i,t)$ $(i = 1, \ldots, r)$ such that $\tilde{p}(t\eta)/(B(\Delta t\eta)^{N/2})$ and $\tilde{q}(t\eta)/(B(\Delta t\eta)^{N/2})$ are in O_K.
(10) For every $t \in M$ let $\Theta(t) = \{\epsilon_1^{\tau(1,t)z_1} \cdots \epsilon_r^{\tau(r,t)z_r} / z_1, \ldots, z_r \in \mathbb{Z}\}$. The elements of $C(O_K)$ are the points computed in Steps 1 and the pairs

$$\left(\frac{\tilde{p}(t\eta\epsilon)}{B(\Delta t\eta\epsilon)^{N/2}}, \frac{\tilde{q}(t\eta\epsilon)}{B(\Delta t\eta\epsilon)^{N/2}} \right)$$

where $\eta \in H(t)$ and $\epsilon \in \Theta(t)$.

Proof of correctness. Suppose that C has a simple point over K. Then there are homogeneous polynomials $u(S,T)$ $v(S,T)$ and $w(S,T)$ in $O_K[S,T]$ of the same degree with no common non-constant factor such that the correspondence

$$(S,T) \longmapsto (u(S,T), v(S,T), w(S,T))$$

defines a birational map $\phi : \mathbb{P}^1 \to \tilde{C}$ over K. By Lemma 2, ϕ is a birational morphism of $\mathbb{P}^1$ onto $\tilde{C}$, $\deg u(S,T) = \deg v(S,T) = \deg w(S,T) = N$ and $w(S,T) = k(aS^2 + bST + cT^2)^{N/2}$, where $\delta = b^2 - 4ac$ is not a square in K.

Let $L = K(\sqrt{\delta})$ and O_L its ring of integers. We put $Z = 2aS + (b + \sqrt{\delta})T$, $W = 2aS + (b - \sqrt{\delta})T$ and so, we obtain the birational morphism $\omega : \mathbb{P}^1 \to \tilde{C}$ over L given by the correspondence

$$(Z,W) \longmapsto (p(Z,W), q(Z,W), A2^N \delta^{N/2} (ZW)^{N/2}),$$

where

$$p(Z,W) = u((b+\sqrt{\delta})W - (b-\sqrt{\delta})Z, 2a(Z-W))$$
$$q(Z,W) = v((b+\sqrt{\delta})W - (b-\sqrt{\delta})Z, 2a(Z-W)).$$

Let $(x,y) \in K^2$ be a non-singular point of C. By Lemma 2, there exist $r, s \in O_K \setminus \{0\}$ such that

$$x = \frac{u(s,t)}{w(s,t)} = \frac{p(2as+(b+\sqrt{\delta}t), 2as+(b-\sqrt{\delta}t))}{A2^N\delta^{N/2}((2as+(b+\sqrt{\delta}t)(2as+(b-\sqrt{\delta}t))^{N/2}},$$
$$y = \frac{v(r,s)}{w(s,t)} = \frac{p(2as+(b+\sqrt{\delta}t), 2as+(b-\sqrt{\delta}t))}{A2^N\delta^{N/2}((2as+(b+\sqrt{\delta}t)(2as+(b-\sqrt{\delta}t))^{N/2}}.$$

Setting $\xi = (2as+(b+\sqrt{\delta}t))/(2as+(b-\sqrt{\delta}t))$, we get

$$x = \frac{p(\xi,1)}{A2^N\delta^{N/2}\xi^{N/2}}, \qquad y = \frac{q(\xi,1)}{A2^N\delta^{N/2}\xi^{N/2}}.$$

Let σ be the K-automorphism of L which is not the identity. Then ξ satisfies $\sigma(\xi) = 1/\xi$. Conversely, suppose that $\xi \in L$ with $\sigma(\xi) = 1/\xi$. Thus, the point (x,y) corresponding to the parameter ξ is defined over L and we have

$$\begin{aligned}(\sigma(x),\sigma(y)) &= \left(\frac{\sigma(p)(1/\xi,1)}{A2^N\delta^{N/2}(1/\xi)^{N/2}}, \frac{\sigma(q)(1/\xi,1)}{A2^N\delta^{N/2}(1/\xi)^{N/2}}\right)\\ &= \left(\frac{p(\xi,1)}{A2^N\delta^{N/2}\xi^{N/2}}, \frac{q(\xi,1)}{A2^N\delta^{N/2}\xi^{N/2}}\right) = (x,y),\end{aligned}$$

whence $(x,y) \in K^2$. Therefore, a point $(x,y) \in L^2$ corresponding to the parameter $\xi \in L$ is defined over K if and only if $\sigma(\xi) = 1/\xi$.

We simplify the polynomials giving ω and we have polynomials $\bar{p}(Z,W), \bar{q}(Z,W) \in O_L[Z,W]$ and $B \in O_L$ such that there is $c \in O_L$ with $p(Z,W) = c\bar{p}(Z,W)$, $q(Z,W) = c\bar{q}(Z,W)$ and $A2^N\delta^{N/2} = Bc$.

Suppose now that $(x,y) \in O_K^2$ and $\xi \in L$ such that

$$x = \frac{\bar{p}(\xi,1)}{B\xi^{N/2}}, \qquad y = \frac{\bar{q}(\xi,1)}{B\xi^{N/2}}.$$

We have

$$\bar{p}(T,1) = \sum_{i=0}^{N} c_i T^{N-i}, \qquad \bar{q}(T,1) = \sum_{i=0}^{N} d_i T^{N-i},$$

where $c_0, \ldots, c_N, d_0, \ldots, d_N \in O_L$. Since $x, y \in O_K$, it follows that $c_0\xi \in O_L$ and $d_0\xi \in O_L$.

Let $c_0 = \delta_1 A_1$ and $d_0 = \delta_2 A_2$, where $\delta_1, \delta_2 \in \mathbb{Z}$ and $A_i = 1$ or $A_i \notin \mathbb{Q}$ $(i = 1,2)$. Thus, if $L_i = \mathbb{Q}(A_i)$ $(i = 1,2)$ and $\Delta = \gcd(\delta_1 N_{L_1}(A_1), \delta_2 N_{L_2}(A_2))$, then $\Delta t \in O_L$. We set $\tilde{\xi} = \Delta\xi$, $\tilde{p}(T) = \bar{p}(T,\Delta)$ and $\tilde{q}(T) = \bar{q}(T,\Delta)$. Since $\sigma(\xi) = 1/\xi$, we have $\sigma(\tilde{\xi}) = \sigma(\Delta\xi) = \Delta/\xi = \Delta^2/\tilde{\xi}$. Hence $N_{L/K}(\tilde{\xi}) = \Delta^2$.

Let R be the resultant of $\tilde{p}(T)$ and $\tilde{q}(T)$. Then, there are $f(T), g(T) \in O_L[T]$ such that

$$R = f(T)\tilde{p}(T) + g(T)\tilde{q}(T).$$

We have $x, y \in O_K$ and

$$x = \frac{\tilde{p}(\tilde{\xi})}{B(\Delta\tilde{\xi})^{N/2}}, \qquad y = \frac{\tilde{q}(\tilde{\xi})}{B(\Delta\tilde{\xi})^{N/2}}.$$

Thus, $B(\Delta\tilde{\xi})^{N/2} | \tilde{p}(\tilde{\xi})$ and $B(\Delta\tilde{\xi})^{N/2} | \tilde{q}(\tilde{\xi})$, and so, we get $N_L(B\Delta^{N/2}) | N_L(R)$.

We denote by G the subgroup of O_L^* consisting of $\eta \in O_L^*$ with $N_{L/K}(\eta) = 1$ and M a maximal set of pairwise non associate elements $z \in O_L$ such that $N_{L/K}(z) = \Delta^2$. Then $\tilde{\xi} = z\eta$, where $z \in M$ and

$\eta \in G$. Finally, reasoning as in the proof of correctness of the previous algorithm we conclude the proof.

As in the algorithm INTEGRAL-POINTS2A, the steps of this algorithm can be achieved by the computational systems KASH, MAGMA and MAPLE.

Example 3. Let a be an algebraic integer such that $a^3 - a - 2 = 0$ and let

$$\begin{aligned} F(X,Y) &= X^4 + 6Y^2X^2 + 9Y^4 - 4X^3 - (32 + 32a + 16a^2)YX^2 - 12Y^2X \\ &\quad + 6X^2 + (64 + 64a + 32a^2)YX + 6Y^2 - 4X - (32 + 32a + 16a^2)Y + 1. \end{aligned}$$

The solutions of the equation $F(X,Y) = 0$ in algebraic integers of $\mathbb{Q}(a)$ are the pairs $(1,0)$ and $(\alpha(t)/12t^2, \beta(t)/12t^2)$, where

$$\begin{aligned} \alpha(T) &= (a^2 + 2a + 2)\sqrt{-3}T^4 + (4a^2 + 8a + 8)\sqrt{-3}T^3 \\ &\quad + 12T^2 - (16a^2 + 32a + 32)\sqrt{-3}T - (16a^2 + 32a + 32)\sqrt{-3}, \\ \beta(T) &= -(a^2 + 2a + 2)T^4 + (8a^2 + 16a + 16)T^2 - 16a^2 - 32a - 32 \end{aligned}$$

and

$$t = 2\left(\frac{1-\sqrt{-3}}{2}\right)^i \left(\frac{(-a^2 + 2a - 1)\sqrt{-3} - 3a^2 + 5}{2}\right)^j, \quad (i = 0, \ldots, 5,\ j \in \mathbb{Z}).$$

Proof. The ring of integers of $K = \mathbb{Q}(a)$ is $\mathbb{Z}[a]$. We denote by C the affine curve defined by $F(X,Y) = 0$. The point $(1,0)$ is the only singular point of C. A parametrization of the corresponding projective curve $\tilde{C}$ is given by the birational morphism

$$\phi : \mathbb{P}^1 \longrightarrow \tilde{C},\ (s:t) \longmapsto (u(s,t) : v(s,t) : w(s,t)),$$

where

$$\begin{aligned} u(s,t) &= s^4 - (32 + 32a + 16a^2)s^3t + 6s^2t^2 + 9t^4, \\ v(s,t) &= 16(2 + 2a + a^2)s^2t^2, \\ w(s,t) &= (s^2 + 3t^2)^2. \end{aligned}$$

Setting $x = s + \sqrt{-3}t$ and $y = s - \sqrt{-3}t$, we obtain the birational morphism

$$\omega : \mathbb{P}^1 \longrightarrow \tilde{C},\ (x:y) \longmapsto (p(x,y) : q(x,y) : 3(xy)^2),$$

where

$$\begin{aligned} p(x,y) &= (a^2 + 2a + 2)\sqrt{-3}x^4 + (2a^2 + 4a + 4)\sqrt{-3}x^3y \\ &\quad + 3x^2y^2 - (2a^2 + 4a + 4)\sqrt{-3}xy^3 - (a^2 + 2a + 2)\sqrt{-3}y^4 \end{aligned}$$

and

$$q(x,y) = -(a^2 + 2a + 2)x^4 + (2a^2 + 4a + 4)x^2y^2 - (a^2 + 2a + 2)y^4.$$

Put $L = K(\sqrt{-3})$. Since $N_K(a^2 + 2a + 2) = 2$, we get

$$\Delta = \gcd(N_L(\sqrt{-3}(a^2 + 2a + 2)), N_K(2 + 2a + a^2)) = 2.$$

We consider the polynomials

$$\begin{aligned} \alpha(T) &= (a^2 + 2a + 2)\sqrt{-3}T^4 + (2a^2 + 4a + 4)2\sqrt{-3}T^3 \\ &\quad + 2^2 3T^2 - (2a^2 + 4a + 4)2^3\sqrt{-3}T - (a^2 + 2a + 2)2^4\sqrt{-3} \end{aligned}$$

and

$$\beta(T) = -(a^2 + 2a + 2)T^4 + (2a^2 + 4a + 4)2^2T^2 - (a^2 + 2a + 2)2^4.$$

Their resultant is $R = 2^{16}3^4(a^2 + 2a + 2)^4$. Since $N_L(12)|N_L(R)$, we proceed to the next steps of our algorithm.

Next, the algorithm RELATIVE-UNITS gives the following basis of G:

$$\zeta = \frac{1-\sqrt{-3}}{2}, \qquad b = \frac{(-a^2+2a-1)\sqrt{-3}-3a^2+5}{2}.$$

A maximal set of pairwise non associate elements $z \in O_L$ such that $N_{L/K}(z) = 4$ is given by 2. The order of the image of b in $(O_K/(48))^*$ is 48. Finally, we find out that the values $\alpha(T)/12T^2$, $\beta(T)/12T^2$ where $T = 2\zeta^i b^j$ $(i = 0, \ldots, 5,\ j = 0, \ldots, 47)$ are elements of O_K. The result follows. □

6. Curves with $|\Sigma_\infty| = 1$

In this section we suppose that the curve C has $|\Sigma_\infty| = 1$. The following algorithm computes the integral solutions of $F(X, Y) = 0$ over K.

The Algorithm INTEGRAL-POINTS1

Input: $C : F(X, Y) = 0$ with $|\Sigma_\infty| = 1$.
Output: The elements of $C(O_K)$.

(1) Determine the singular points of $C(O_K)$.
(2) Find homogeneous polynomials $p(U, V), q(U, V) \in O_K[U, V]$ of degree N and $d \in O_K \setminus \{0\}$ such that the correspondence

$$(U, V) \longmapsto (p(U, V), q(U, V), dU^N),$$

defines a birational morphism $\psi : \mathbb{P}^1 \to \tilde{C}$ over K. If there are no such polynomials, then $C(O_K)$ contains only the points obtained in Step 1. Else, go to the next step.
(3) Let a and b be the leading coefficients of $p_1(V) = p(1, V)$ and $q_1(V) = q(1, V)$ respectively. If $a = a'A_1$ and $b = b'A_2$, where $a', b' \in \mathbb{Z}$ and $A_i = 1$ or $A_i \notin \mathbb{Q}$ $(i = 1, 2)$, then compute $\delta = \gcd(a'N_K(A_1), b'N_K(A_2))$.
(4) Compute the polynomials

$$p_2(T) = (\delta D)^{\deg p_1} p_1(T/\delta D), \qquad q_2(T) = (\delta D)^{\deg q_1} q_1(T/\delta D),$$

where $D = 1$ if $d \in \mathbb{Z}$ and $D = N_K(d)/d$ otherwise. Set $\hat{d} = d$, if $d \in \mathbb{Z}$ and $\hat{d} = N_K(d)$ otherwise.
(5) Compute the resultant R of polynomials $p_2(T)$ and $q_2(T)$. If $\hat{d}\delta^m \not| R$, where $m = \min\{\deg p_1, \deg q_1\}$, then all the elements of $C(O_K)$ are those computed in Step 1. Otherwise, go to the next step.
(6) Determine the set S of elements $t \in O_K$ satisfying

$$p_2(t) \equiv 0 \pmod{\hat{d}\delta^{\deg p_2}}, \qquad q_2(t) \equiv 0 \pmod{\hat{d}\delta^{\deg q_2}}.$$

(7) The elements of $C(O_K)$ are the points computed in Step 1 and the pairs (x, y) given by

$$x = \frac{p_2(t)}{\hat{d}\delta^{\deg p_2}}, \qquad y = \frac{q_2(t)}{\hat{d}\delta^{\deg q_2}}, \quad t \in S.$$

Proof of correctness. Suppose that C has a simple point over K. Then there are homogeneous polynomials $u(S, T)$ $v(S, T)$ and $w(S, T)$ in $O_K[S, T]$ of the same degree with no common non-constant factor such that the correspondence

$$(S, T) \longmapsto (u(S, T), v(S, T), w(S, T))$$

defines a birational map $\phi : \mathbb{P}^1 \to \tilde{C}$ over K. By Lemma 2, we have that ϕ is a birational morphism of $\mathbb{P}^1$ onto $\tilde{C}$, $\deg u(S, T) = \deg v(S, T) = \deg w(S, T) = N$ and $w(S, T) = a(bS+cT)^N$. Put $U = bS+cT$ and $V = S$. Then we have a birational morphism $\psi : \mathbb{P}^1 \to \tilde{C}$ over K given by the correspondence

$$(U, V) \longmapsto (p(U, V), q(U, V), dU^N),$$

where $p(U, V)$ and $q(U, V)$ are homogeneous polynomials in $O_K[U, V]$ of degree N and $d \in O_K \setminus \{0\}$.

Let $(x, y) \in C(O_K)$ be a non-singular point. By Lemma 2, there are $s, t \in O_K$ such that $x = p(s,t)/ds^N$ and $y = q(s,t)/ds^N$. Setting $p_1(V) = p(1,V)$, $q_1(V) = q(1,V)$ and $\tau = t/s$, we get $x = p_1(\tau)/d$ and $y = q_1(\tau)/d$.

Let a and b be the leading coefficients of $p_1(V)$ and $q_1(V)$ respectively. Since $x, y \in O_K$, it follows that $a\tau, b\tau \in O_K$. Let $a = a'A_1$ and $b = b'A_2$, where $a', b' \in \mathbb{Z}$ and $A_i = 1$ or $A_i \notin \mathbb{Q}$ $(i = 1, 2)$, and $\delta = \gcd(a'N_K(A_1), b'N_K(A_2))$. We have that $a'N_K(A_1)\tau$ and $b'N_K(A_2)\tau$ are in O_K, and so $\delta\tau \in O_K$.

Suppose that $p_1(T) = a_0T^\mu + \cdots + a_\mu$ and $q_1(T) = b_0T^\nu + \cdots + b_\nu$. Further, let $D \in O_K$ be such that $Dd = \hat{d} \in \mathbb{Z}$ ($D = 1, \hat{d} = d$, if $d \in \mathbb{Z}$ and $\hat{d} = N_K(d)$, $D = N_K(d)/d$, otherwise). We set

$$p_2(T) = \sum_{i=0}^{\mu} a_i(D\delta)^i T^{\mu-i}, \qquad q_2(T) = \sum_{i=0}^{\nu} b_i(D\delta)^i T^{\mu-i}.$$

Then

$$x = \frac{p_2(\delta\tau)}{\hat{d}\delta^\mu}, \qquad y = \frac{q_2(\delta\tau)}{\hat{d}\delta^\nu}.$$

Let R be the resultant of polynomials $p_2(T)$ and $q_2(T)$. Since $x, y \in O_K$, we deduce that $\hat{d}\delta^m | R$, where $m = \min\{\mu, \nu\}$. Furthermore, $\delta\tau$ satisfies the polynomial congruences

$$p_2(T) \equiv 0 \pmod{\hat{d}\delta^\mu}, \qquad q_2(T) \equiv 0 \pmod{\hat{d}\delta^\nu}.$$

Conversely, if $z \in O_K$ satisfies the above congruences, then the pair

$$\left(\frac{p_2(z)}{\hat{d}\delta^\mu}, \frac{q_2(z)}{\hat{d}\delta^\nu}\right)$$

is an integral solution to the equation $F(X, Y) = 0$.

Example 4. Let

$$F(X, Y) = -2Y^3 + X^2 + 3\sqrt{2}XY + \sqrt{2}X.$$

The solutions of the equation $F(X, Y) = 0$ in $\mathbb{Z}[\sqrt{2}]$ are

$$(X, Y) = (\sqrt{2}, -1), (p(t)/2, q(t)/2),$$

where $t \equiv 1, 1 + \sqrt{2} \pmod 2$ and

$$p(t) = (5\sqrt{2} - 7)t^3 + 2(-6\sqrt{2} + 9)t^2 + 4(3\sqrt{2} - 3)t + 8,$$
$$q(t) = (-2\sqrt{2} + 3)t^2 + 2\sqrt{2}t + 4(\sqrt{2} + 1).$$

Proof. Denote by C the affine curve defined by $F(X, Y) = 0$. The ring of integers of $K = \mathbb{Q}(\sqrt{2})$ is $\mathbb{Z}[\sqrt{2}]$. The point $(\sqrt{2}, -1)$ is its only singular point of C. A parametrization of the corresponding projective curve $\tilde{C}$ is given by the birational morphism

$$\phi : \mathbb{P}^1 \longrightarrow \tilde{C}, \ (s : t) \longmapsto (u(s,t) : v(s,t) : w(s,t)),$$

where

$$u(s,t) = (5\sqrt{2} - 7)t^3 + (-6\sqrt{2} + 9)t^2s + (3\sqrt{2} - 3)ts^2 + s^3,$$
$$v(s,t) = (-2\sqrt{2} + 3)t^2s + \sqrt{2}ts^2 + (\sqrt{2} + 1)s^3,$$
$$w(s,t) = 2s^3.$$

We have $\gcd(N_K(5\sqrt{2} - 7), N_K(-2\sqrt{2} + 3)) = 1$. The resultant of $u(1, T)$ and $v(1, T)$ is zero. Thus, we continue to the next step of our algorithm. Now, we shall determine the set S of elements $t \in O_K$ satisfying

$$(5\sqrt{2} - 7)t^3 + (-6\sqrt{2} + 9)t^2 + (3\sqrt{2} - 3)t + 1 \equiv 0 \pmod 2,$$
$$(-2\sqrt{2} + 3)t^2 + \sqrt{2}t + (\sqrt{2} + 1) \equiv 0 \pmod 2.$$

Setting $t = x + y\sqrt{2}$, where $x, y \in \mathbb{Z}$, we deduce the following system:

$$x^3 + x^2y + x + y \equiv 0 \pmod 2, \qquad x^3 + x^2 + x + 1 \equiv 0 \pmod 2,$$
$$x + 1 \equiv 0 \pmod 2, \qquad x^2 + 1 \equiv 0 \pmod 2.$$

It follows that $(x, y) \equiv (1, 0), (1, 1) \pmod 2$, whence $t \equiv 1, 1 + \sqrt{2} \pmod 2$. The non-singular integral points of C are given by $(p(t)/2, q(t)/2)$, where $t \equiv 1, 1 + \sqrt{2} \pmod 2$ and

$$p(t) = (5\sqrt{2} - 7)t^3 + 2(-6\sqrt{2} + 9)t^2 + 4(3\sqrt{2} - 3)t + 8,$$
$$q(t) = (-2\sqrt{2} + 3)t^2 + 2\sqrt{2}t + 4(\sqrt{2} + 1). \quad \square$$

Acknowledgements

The research of the first author was financial supported by Hellenic State Scholarships Foundation-I.K.Y. The computations were carried out with the Transnational Access Programme at RISC, Johannes Kepler University Linz, supported by the European Commission Framework 6 Programme for Integrated Infrastructures Initiatives under the project SCIEnce (contract No. 026133). The authors are duly grateful to RISC for providing access to this programme. Moreover, the authors thank the referees for helpful comments and suggestions.

References

Alvanos, P., Bilu, Y., Poulakis, D., 2009. Characterizing algebraic curves with infinitely many integral points. Internat. J. Number Theory 5 (4), 585–590.
Gaál, I., Pohst, M., 2002. On the resolution of relative Thue equations. Math. Comp. 71, 429–440.
Hess, F., 2002. Computing Riemann–Roch spaces in algebraic function fields and related topics. J. Symbolic Comput. 33, 425–445.
Lang, S., 1978. Elliptic Curves. Diophantine Analysis. Springer-Verlag, Berlin, Heidelberg, New-York.
Lang, S., 1983. Fundamentals of Diophantine Geometry. Springer-Verlag, New-York, Berlin, Heidelberg, Tokyo.
Maillet, E., 1918. Détermination des points entiers des courbes unicursales à coefficients entiers. C. R. Acad. Paris 168, 217–220.
Maillet, E., 1919. Détermination des points entiers des courbes unicursales à coefficients entiers. J. de l'Ecole Polytechnique 2, 115–156.
Poulakis, D., Voskos, E., 2000. On the practical solution of genus zero Diophantine equations. J. Symbolic Comput. 30 (5), 573–582.
Poulakis, D., Voskos, E., 2002. Solving genus zero Diophantine equations with at most two infinite valuations. J. Symbolic Comput. 33 (4), 479–491.
Schmidt, W.M., 1991. Construction and estimation of bases in function fields. J. Number Theory 39 (2), 181–224.
Wildanger, K., 2000. Über das Lösen von Einheiten- und Indexformgleichungen in algebraischen Zahlkörpern. J. Number Theory 82 (2), 188–224.
http://www.math.tu-berlin.de/~kant/.
http://magma.maths.usyd.edu.au/magma/.